FIG. 1

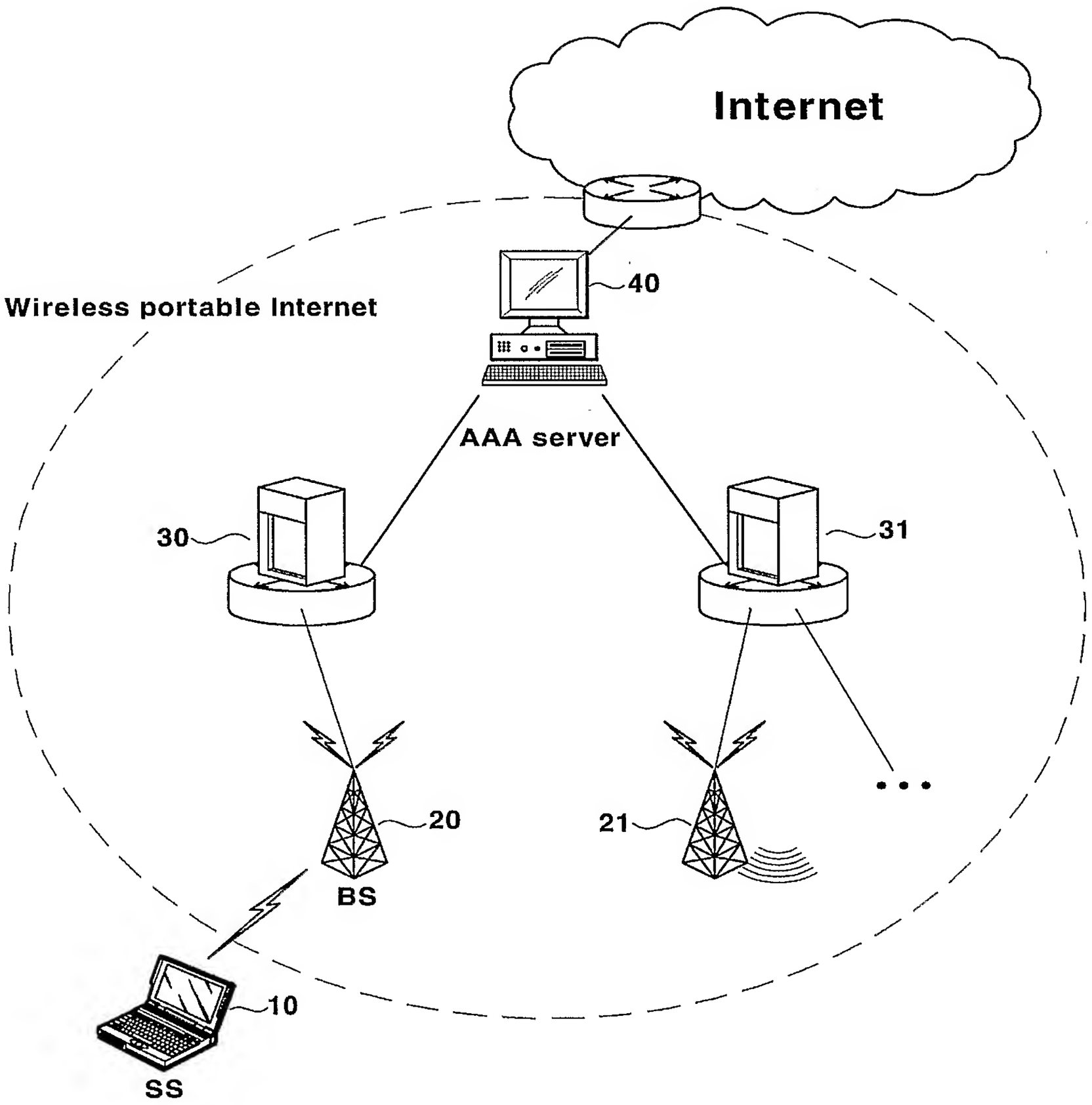

Internet
Wireless portable Internet
40
AAA server
30
31
20
21
BS
10
SS

FIG. 2

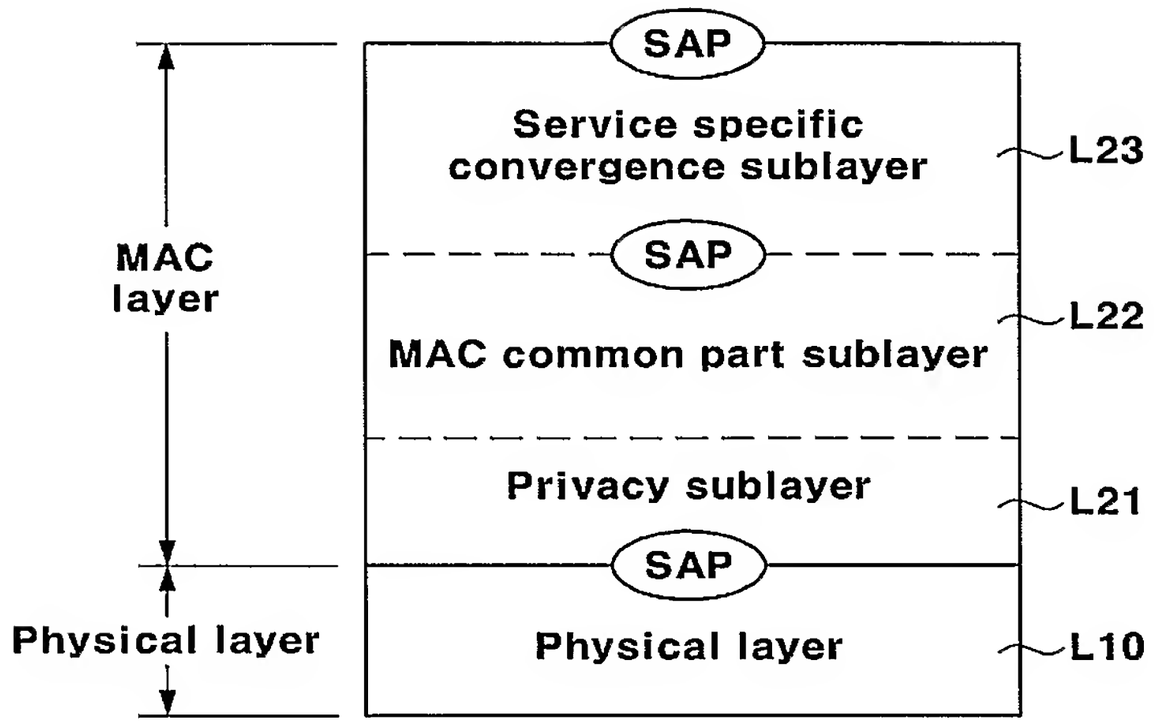

SAP
Service specific convergence sublayer
L23
SAP
MAC common part sublayer
L22
Privacy sublayer
L21
SAP
Physical layer
L10
MAC layer
Physical layer

FIG. 3

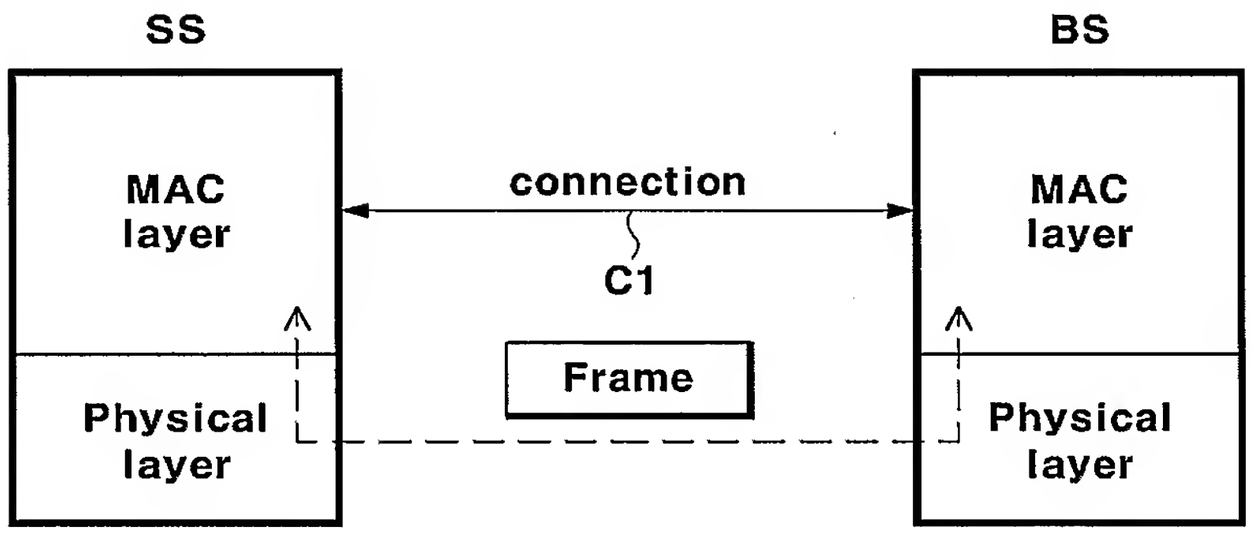

SS
BS
MAC layer
connection
C1
MAC layer
Frame
Physical layer
Physical layer

FIG. 4

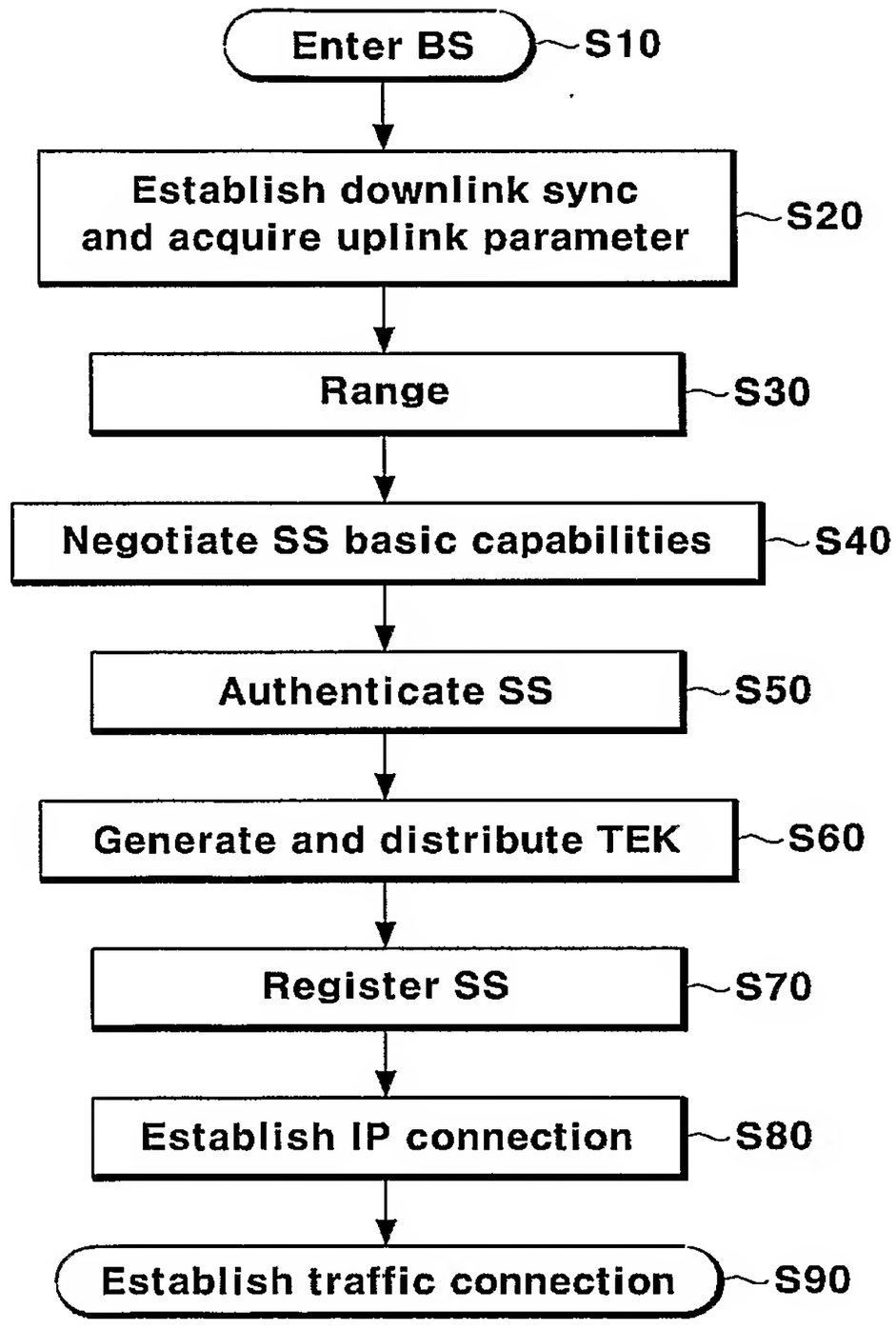
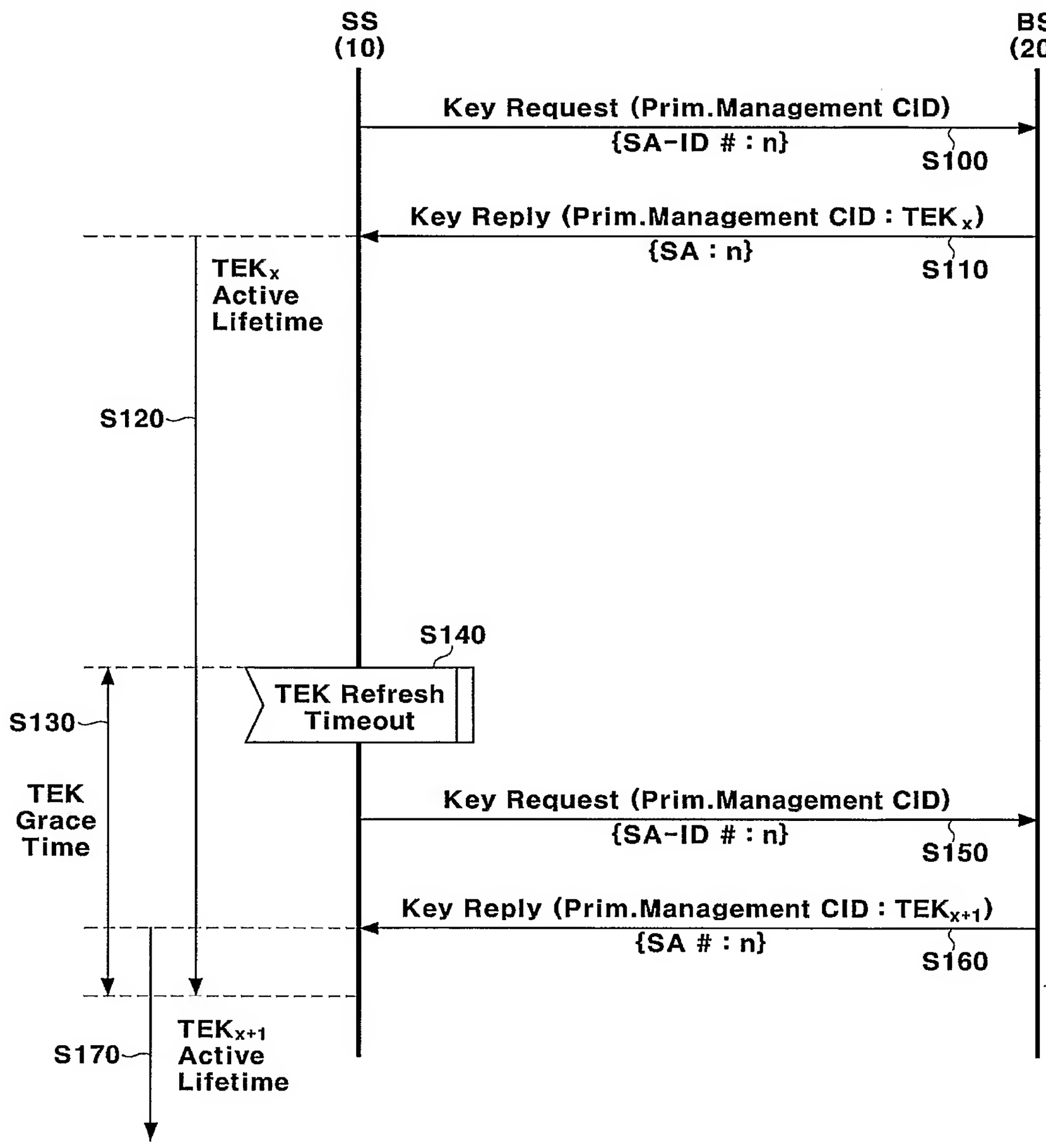

Enter BS
S10
Establish downlink sync and acquire uplink parameter
S20
Range
S30
Negotiate SS basic capabilities
S40
Authenticate SS
S50
Generate and distribute TEK
S60
Register SS
S70
Establish IP connection
S80
Establish traffic connection
S90

FIG. 5


SS
(10)
BS
(20)
Key Request (Prim.Management CID)
{SA-ID # : n}
S100
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S110
TEKx
Active
Lifetime
S120
S140
TEK Refresh
Timeout
S130
TEK
Grace
Time
Key Request (Prim.Management CID)
{SA-ID # : n}
S150
Key Reply (Prim.Management CID : TEKx+1)
{SA # : n}
S160
TEKx+1
Active
Lifetime
S170

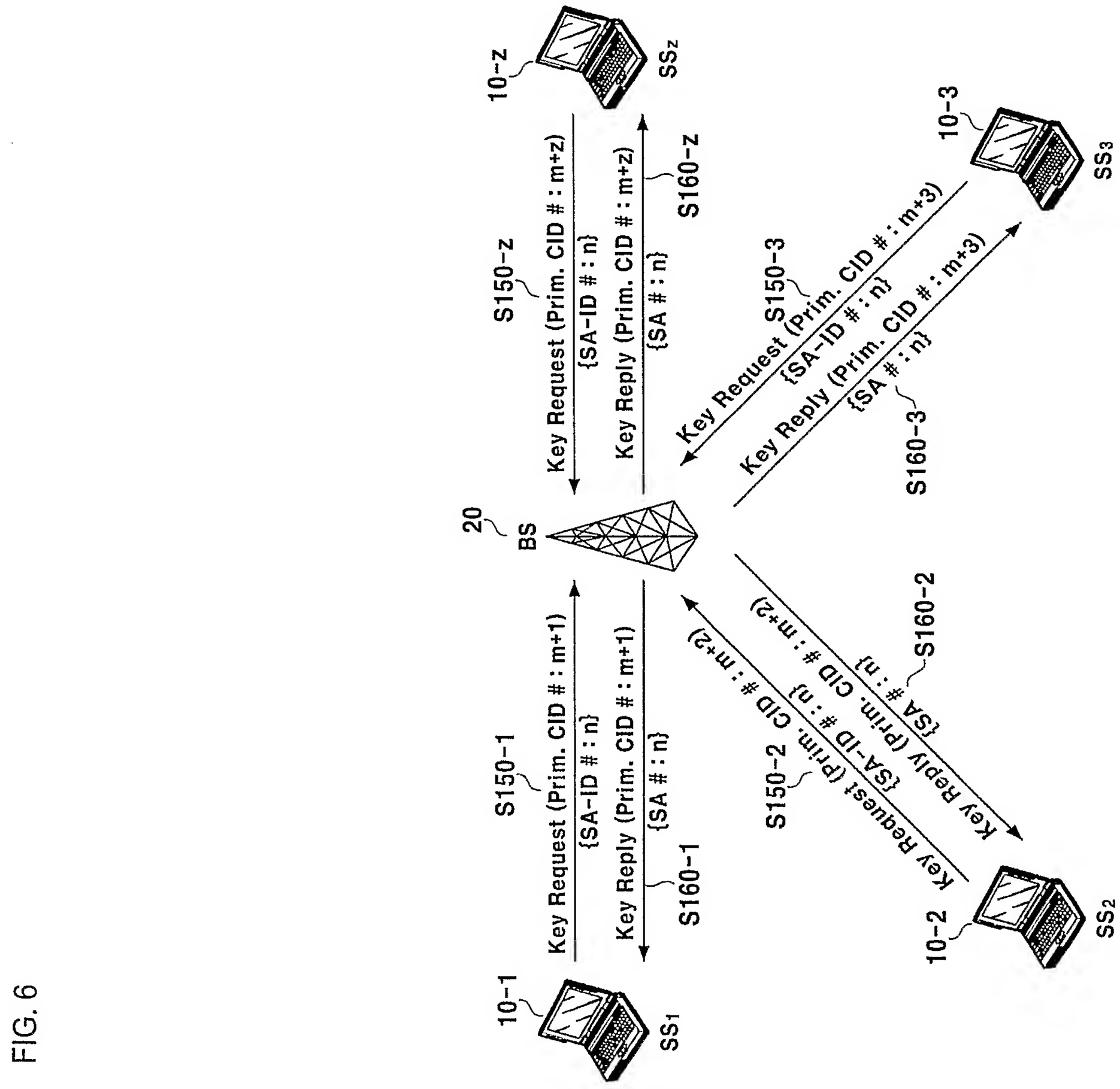

10-z
SSz
S150-z
Key Request (Prim. CID # : m+z)
{SA-ID # : n}
Key Reply (Prim. CID # : m+z)
{SA # : n}
S160-z
10-3
SS3
S150-3
Key Request (Prim. CID # : m+3)
{SA-ID # : n}
Key Reply (Prim. CID # : m+3)
{SA # : n}
S160-3
20
BS
S150-1
Key Request (Prim. CID # : m+1)
{SA-ID # : n}
Key Reply (Prim. CID # : m+1)
{SA # : n}
S160-1
10-1
SS1
S150-2
Key Request (Prim. CID # : m+2)
{SA-ID # : n}
Key Reply (Prim. CID # : m+2)
{SA # : n}
S160-2
10-2
SS2

FIG. 6

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

FIG. 7

FIG. 8

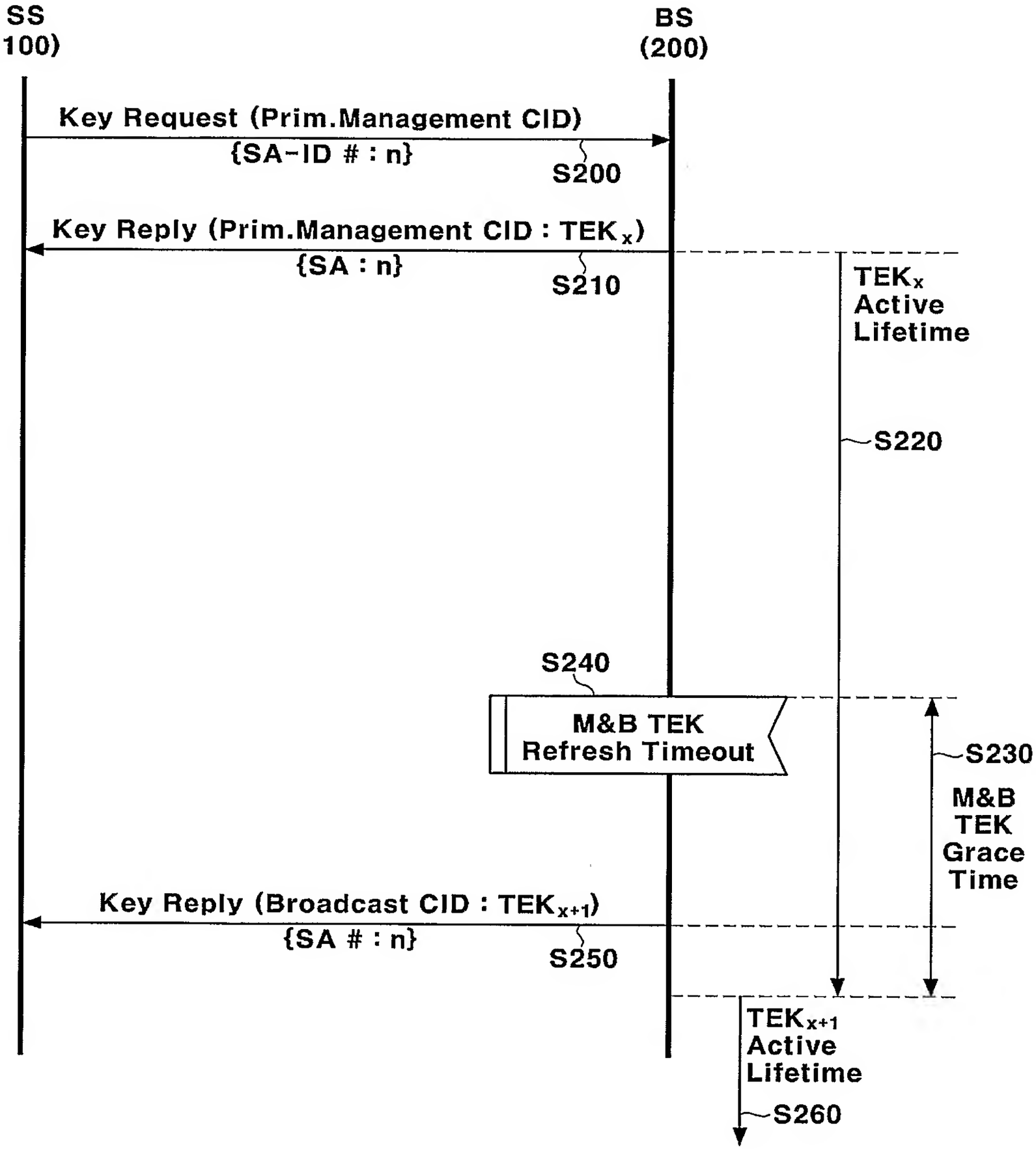
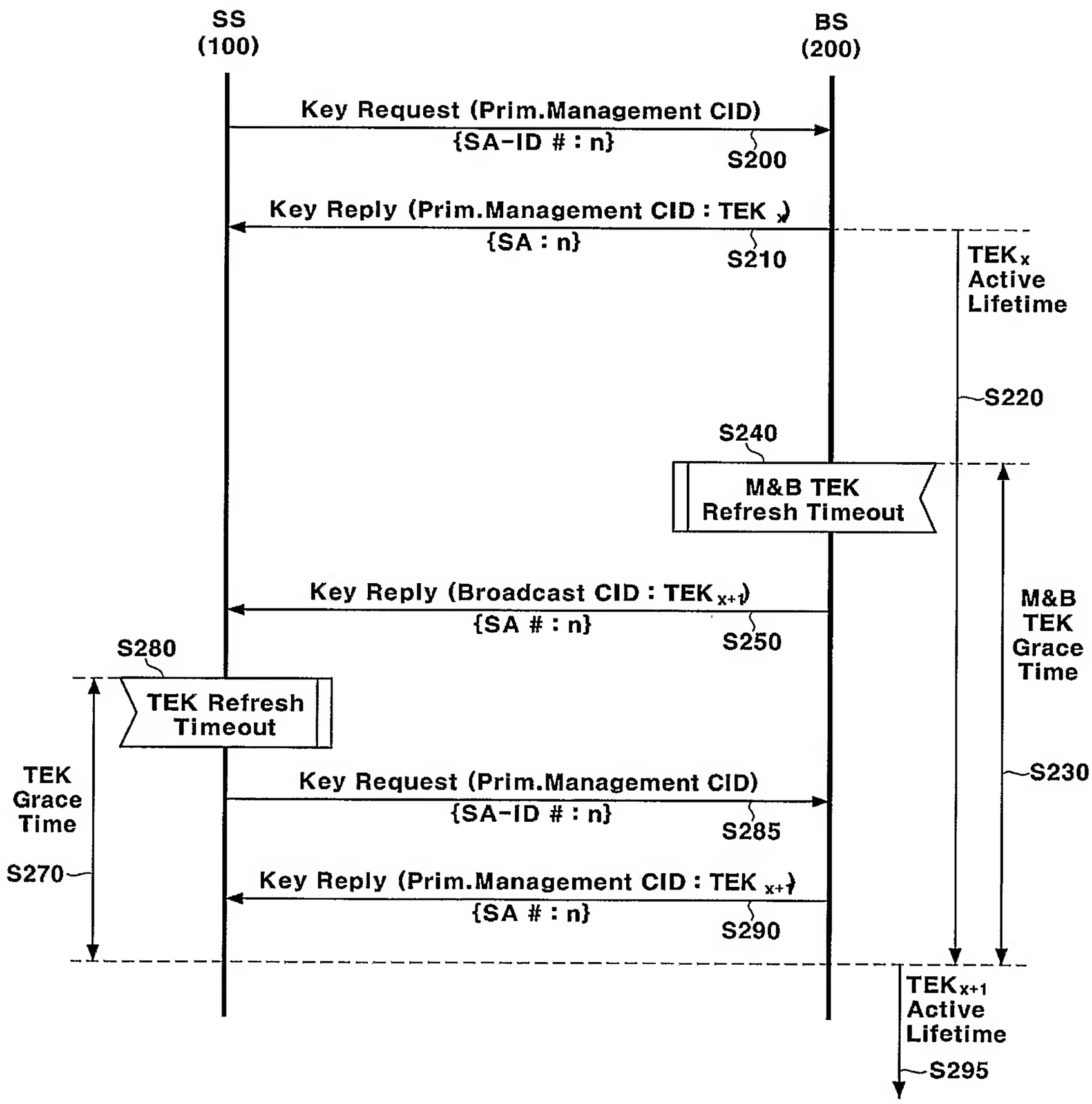

SS
(100)
BS
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S200
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S210
TEKx
Active
Lifetime
S220
S240
M&B TEK
Refresh Timeout
S230
M&B
TEK
Grace
Time
Key Reply (Broadcast CID : TEKx+1)
{SA # : n}
S250
TEKx+1
Active
Lifetime
S260

FIG. 9


SS
(100)
BS
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S200
Key Reply (Prim.Management CID : TEK x)
{SA : n}
S210
TEKx
Active
Lifetime
S220
S240
M&B TEK
Refresh Timeout
Key Reply (Broadcast CID : TEKx+1)
{SA # : n}
S250
M&B
TEK
Grace
Time
S230
S280
TEK Refresh
Timeout
TEK
Grace
Time
S270
Key Request (Prim.Management CID)
{SA-ID # : n}
S285
Key Reply (Prim.Management CID : TEK x+1)
{SA # : n}
S290
TEKx+1
Active
Lifetime
S295

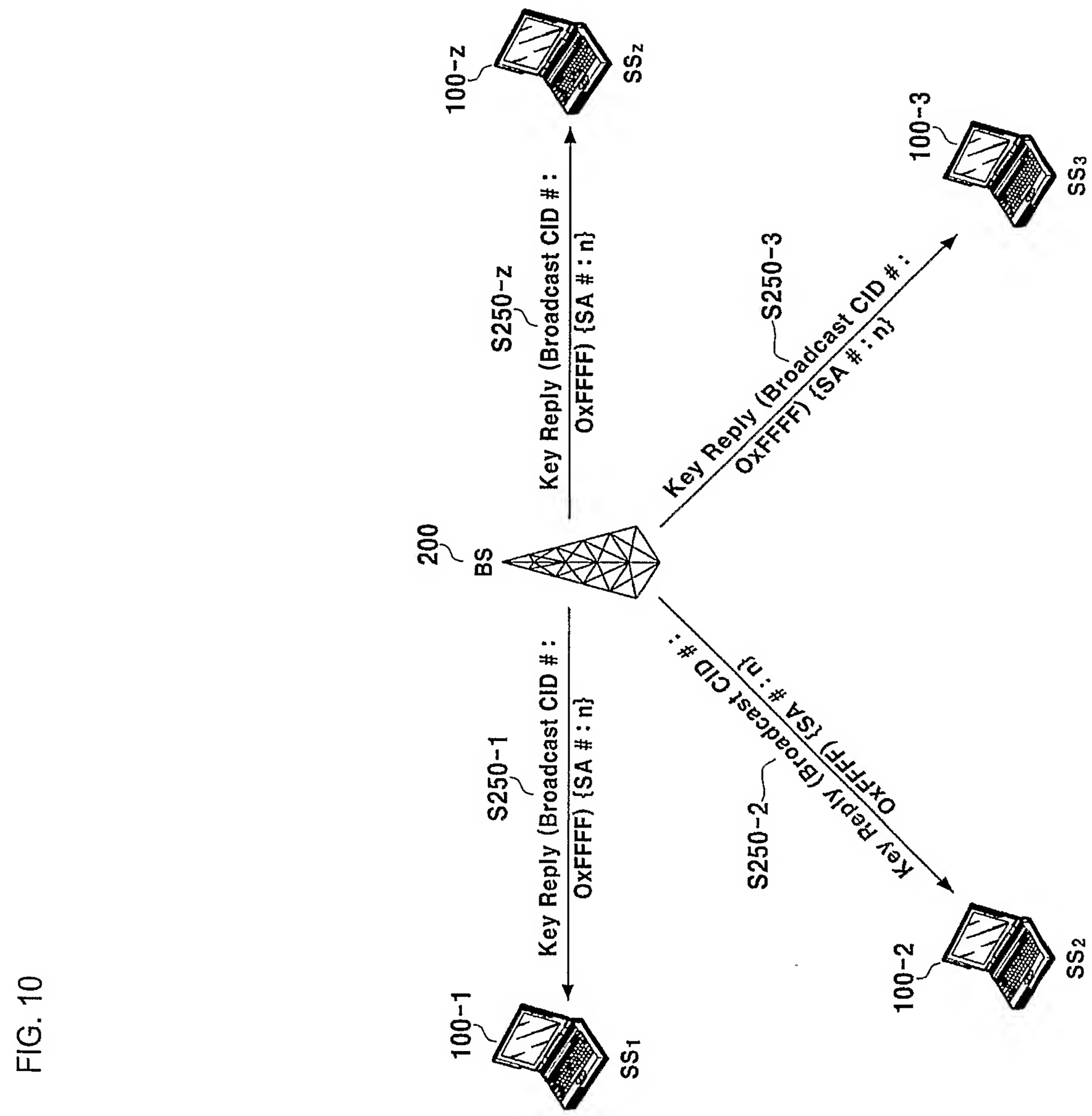
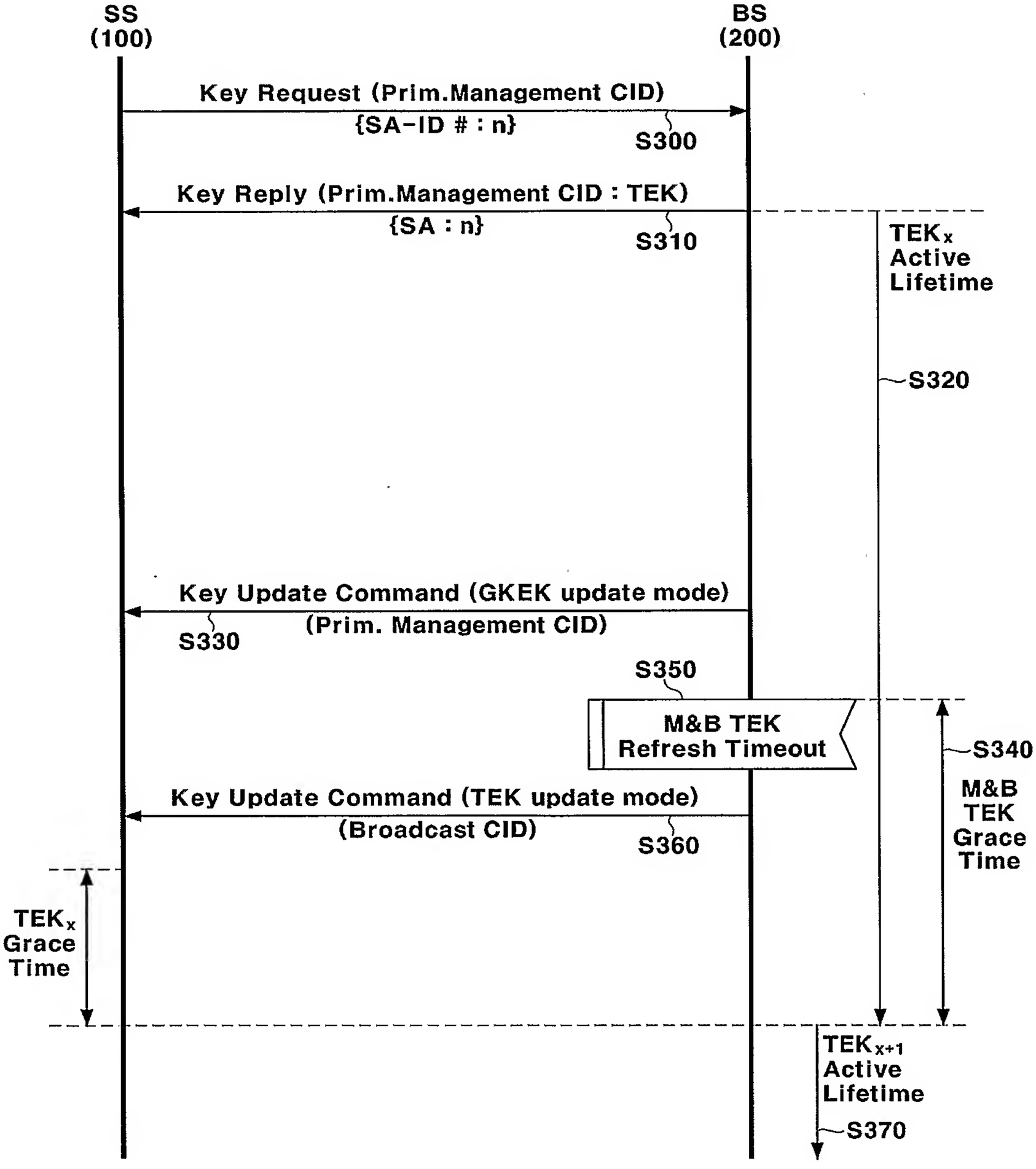

100-z
SSz
S250-z
Key Reply (Broadcast CID # :
OxFFFF) {SA # : n}
200
BS
S250-3
Key Reply (Broadcast CID # :
OxFFFF) {SA # : n}
100-3
SS3
S250-1
Key Reply (Broadcast CID # :
OxFFFF) {SA # : n}
S250-2
Key Reply (Broadcast CID # :
OxFFFF) {SA # : n}
100-1
SS1
100-2
SS2

FIG. 10

FIG. 11

CID(MAC Header)	Key to encrypt the TEK
Primary Management CID	KEK(Derived from the AK)
Broadcast CID	Old distributed TEK

FIG. 12


SS
(100)
BS
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S300
Key Reply (Prim.Management CID : TEK)
{SA : n}
S310
TEKx
Active
Lifetime
S320
Key Update Command (GKEK update mode)
(Prim. Management CID)
S330
S350
M&B TEK
Refresh Timeout
S340
M&B
TEK
Grace
Time
Key Update Command (TEK update mode)
(Broadcast CID)
S360
TEKx
Grace
Time
TEKx+1
Active
Lifetime
S370

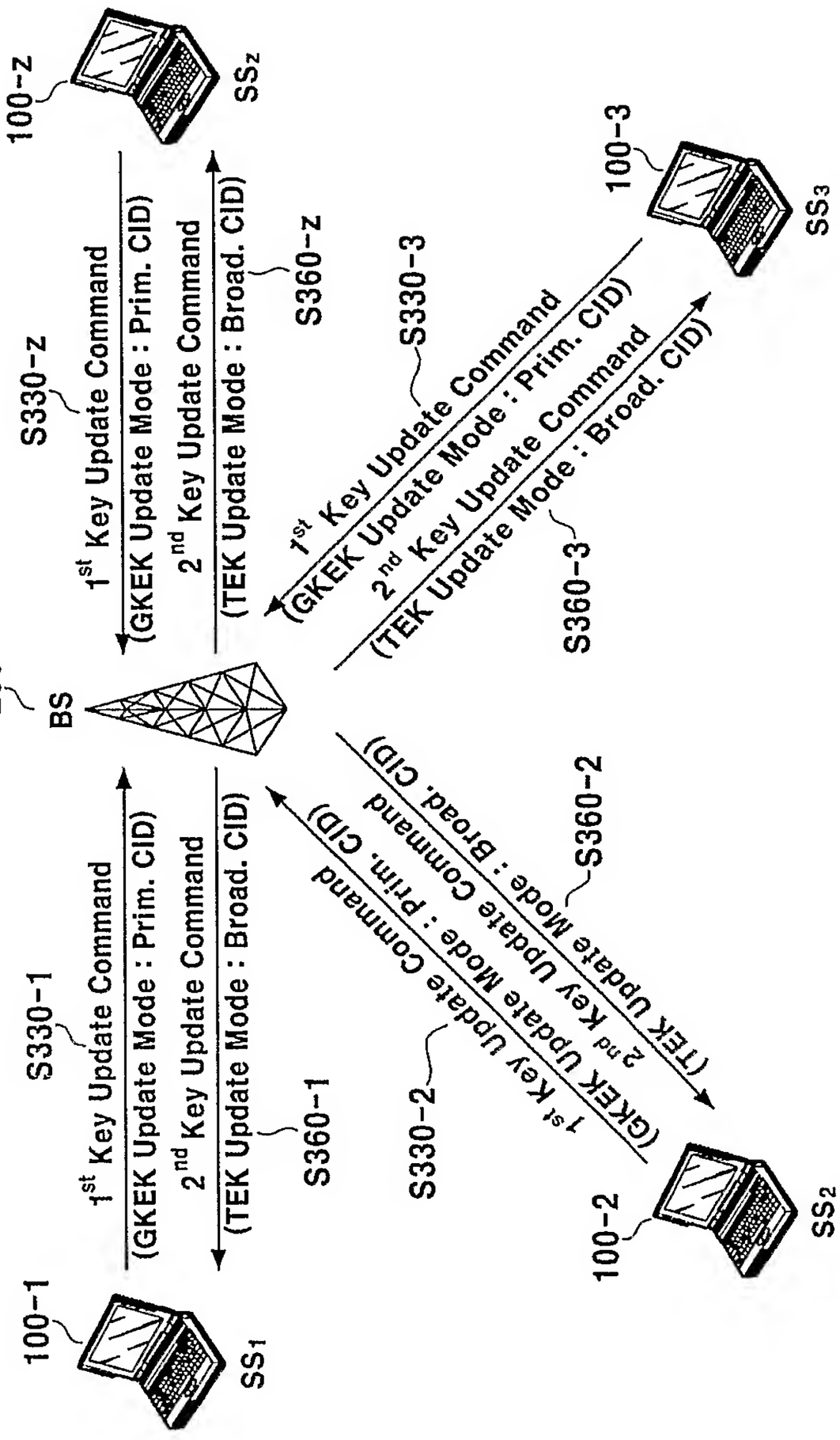

100-z
SSz
100-3
SS3
S330-z
1st Key Update Command
(GKEK Update Mode : Prim. CID)
2nd Key Update Command
(TEK Update Mode : Broad. CID)
S360-z
S330-3
1st Key Update Command
(GKEK Update Mode : Prim. CID)
2nd Key Update Command
(TEK Update Mode : Broad. CID)
S360-3
200
BS
S330-1
1st Key Update Command
(GKEK Update Mode : Prim. CID)
2nd Key Update Command
(TEK Update Mode : Broad. CID)
S360-1
S330-2
1st Key Update Command
(GKEK Update Mode : Prim. CID)
2nd Key Update Command
(TEK Update Mode : Broad. CID)
S360-2
100-1
SS1
100-2
SS2

FIG. 13

FIG. 14

Attributes	Contents
Key-Sequece-Number	Authorization Key sequence number
SAID	Security Association ID
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

FIG. 15

Attributes	Contents
GKEK	GKEK, encrypted with the AK
TEK	TEK, encrypted wity the GKEK (Multicast or Broadcast Service) or encrypted with the KEK (Unicast Service)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

FIG. 16

Attributes	Contents	1st Message (Primary)	2nd Message (Braodcast)
Key-Sequence-Number	Authorization key sequence number	○	○
SAID	Security Association ID	○	○
Key Push Modes	Usage code of Key Update Command message	○	○
Key Push Counter	Counter one greater than that of older generation for reply attack	○	○
TEK-Parameters	"Newer" generation of key parameters relevant to SAID		
> GKEK	GKEK, encrypted with the AK	○	×
> TEK	TEK, encrypted with the GKEK(Multicast or Broadcast Service)	×	○
> Key-Lifetime	TEK Remaining Lifetime	×	○
> Key-Sequence-Number	TEK Sequnce Number	○	○
> CBS-IV	Cipher Block Chaining (CBC) Initialization Vector	×	○
HMAC-Digest	Keyed SHA message digest	○	○

FIG. 17

Type	Length	Value
30	1	0, GKEK update mode (1st Message) 1, TEK update mode (2nd Message) 2-225, reserved

FIG. 18

Key push modes	Input Key
GKEK update mode	AK
TEK update mode	GKEK

FIG. 19

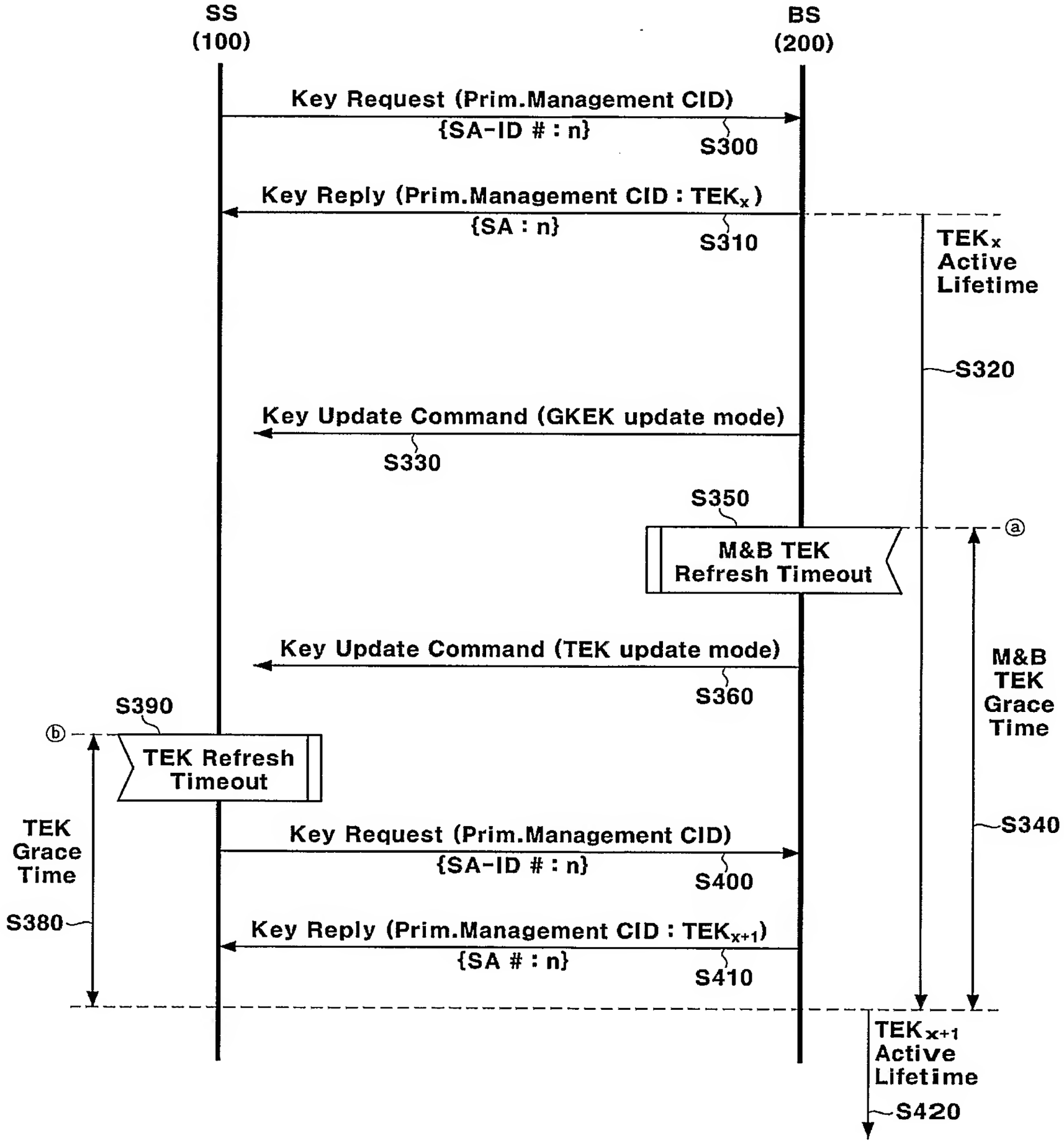

SS
(100)
BS
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S300
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S310
TEKx Active Lifetime
S320
Key Update Command (GKEK update mode)
S330
S350
M&B TEK Refresh Timeout
ⓐ
Key Update Command (TEK update mode)
S360
S390
ⓑ
TEK Refresh Timeout
M&B TEK Grace Time
S340
TEK Grace Time
S380
Key Request (Prim.Management CID)
{SA-ID # : n}
S400
Key Reply (Prim.Management CID : TEKx+1)
{SA # : n}
S410
TEKx+1 Active Lifetime
S420

FIG. 20

Situation	Transferred TEK-parameter information
Initial TEK response (before ⓐ)	TEK-parameters $_C$
Initial TEK response (after ⓐ)	TEK-parameters $_C$ & TEK-parameters $_N$
Initial update response (after ⓑ)	TEK-parameters $_N$

C : Current generation of key parameters relevant to SAID

N : Next generation of key parameters relevant to SAID

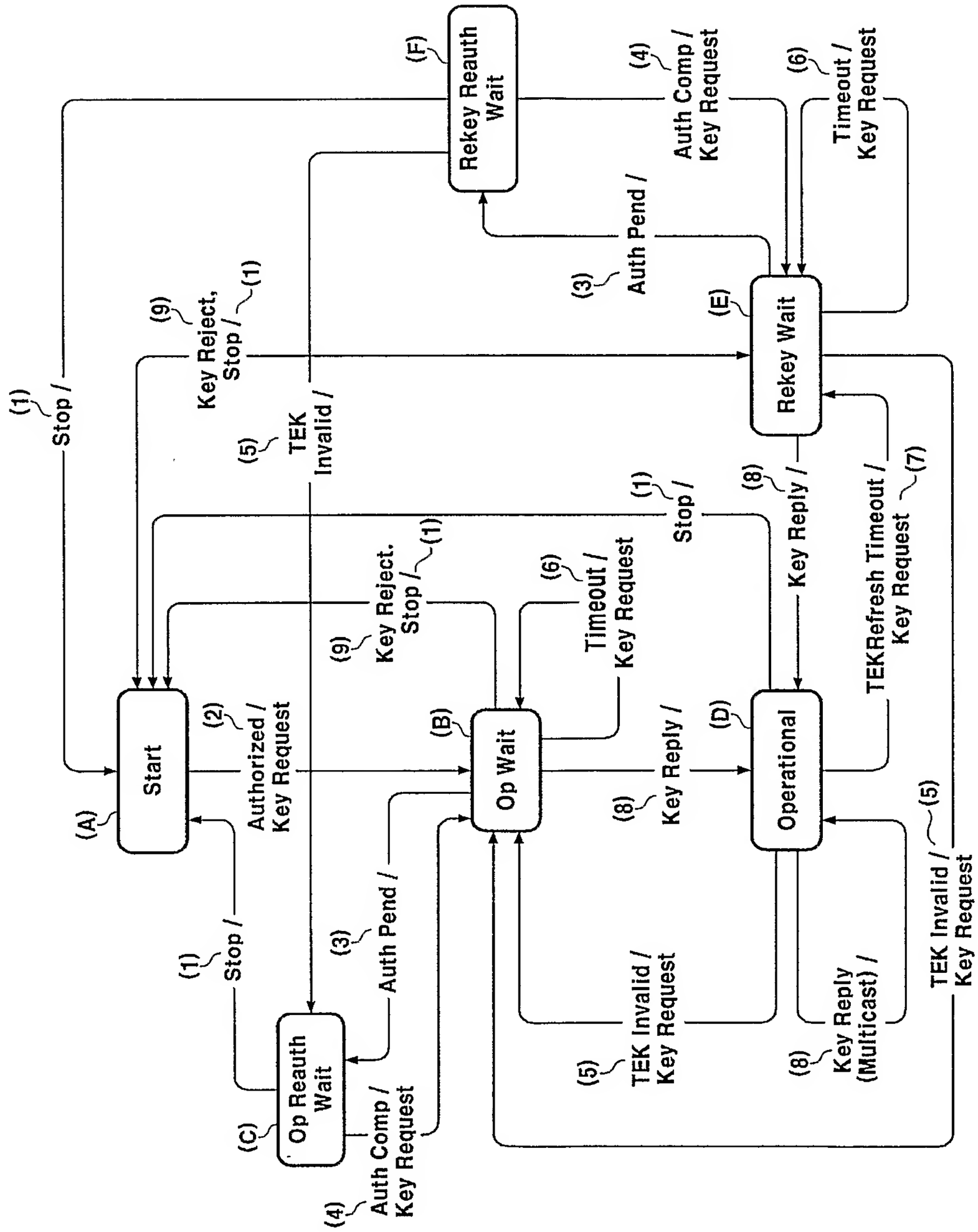

Rekey Reauth Wait
(F)
(4)
Auth Comp / Key Request
(6)
Timeout / Key Request
(3)
Auth Pend /
(E)
Rekey Wait
(9)
Key Reject, Stop /
(1)
(1)
Stop /
(5)
TEK Invalid /
(1)
Stop /
(8)
Key Reply /
(7)
TEKRefresh Timeout / Key Request
(9)
Key Reject. Stop /
(1)
(6)
Timeout / Key Request
Start
(A)
(2)
Authorized / Key Request
(B)
Op Wait
(D)
Operational
(8)
Key Reply /
(5)
TEK Invalid / Key Request
(1)
Stop /
(3)
Auth Pend /
Op Reauth Wait
(C)
(4)
Auth Comp / Key Request
(8)
Key Reply (Multicast) /
TEK Invalid / Key Request

FIG. 21

[Fig. 22]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	

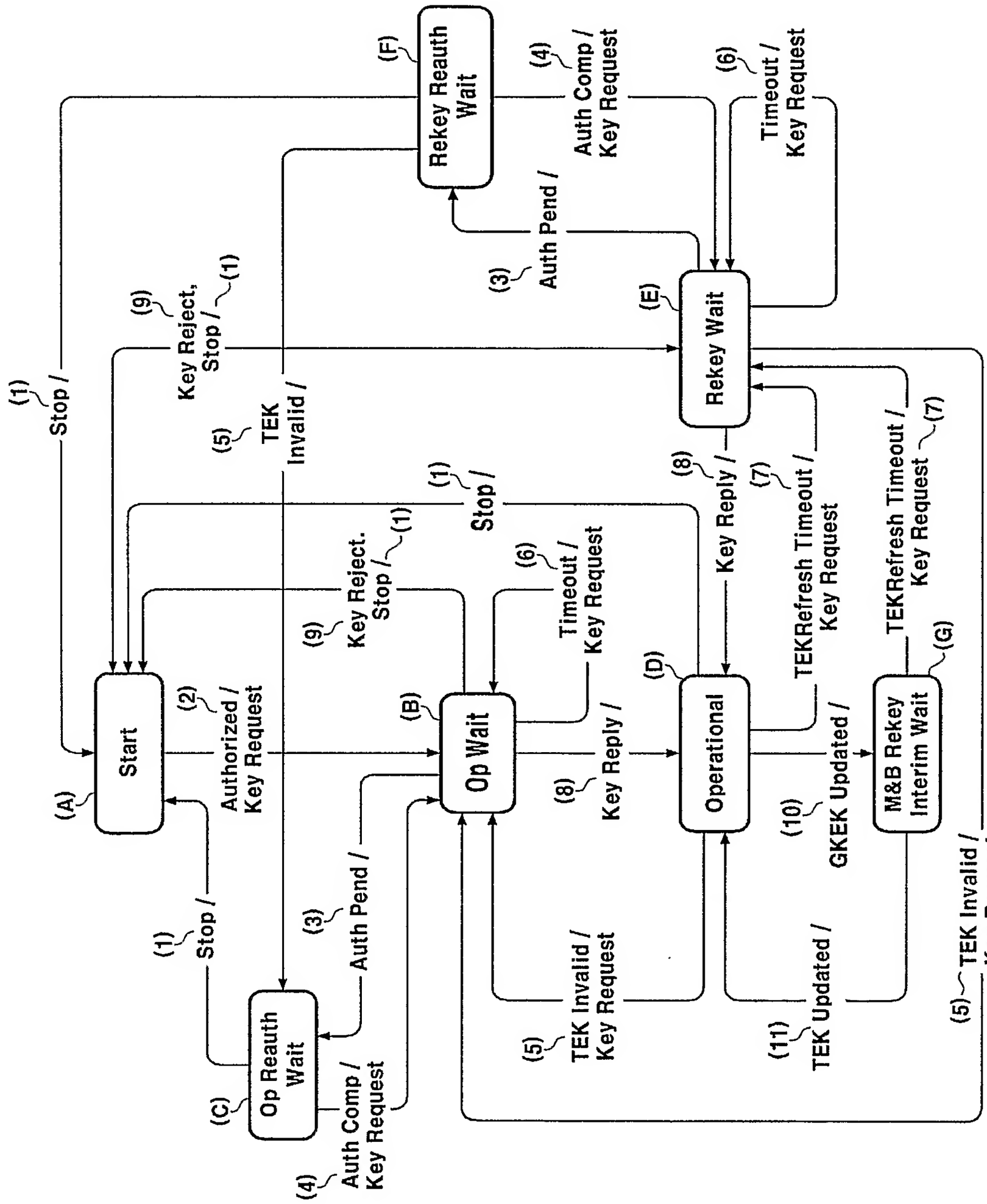

Start
(A)
Op Wait
(B)
Op Reauth Wait
(C)
Operational
(D)
Rekey Wait
(E)
Rekey Reauth Wait
(F)
M&B Rekey Interim Wait
(G)
(1) Stop /
(2) Authorized / Key Request
(3) Auth Pend /
(4) Auth Comp / Key Request
(5) TEK Invalid / Key Request
(6) Timeout / Key Request
(7) TEKRefresh Timeout / Key Request
(8) Key Reply /
(9) Key Reject, Stop /
(10) GKEK Updated /
(11) TEK Updated /

FIG. 23

[Fig. 24]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B rekey Interim Wait
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait	
(6) Timeout		Op Wait			Rekey Wait		
(7) TEK Refresh Timeout				Rekey Wait			Rekey Wait
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start			Start		
(10) GKEK Updated				Rekey Wait			
(11) TEK Updated							Operational